REMARKS

Status of Claims:

Claims 1-22 are present for examination.

Prior Art Rejection:

Claims 1-6, 9, 12, 15 and 18-22 stand rejected under 35 U.S.C. § 102 as anticipated by Ateniese. Further, claims 1-6, 9, 12, 15 and 18-22 stand rejected under 35 U.S.C. § 103 as obvious over Ramzan in view of Ateniese. Claims 7-8 stand rejected under 35 U.S.C. § 103 as obvious over Ateniese in view of Camenisch. Claims 10-11 stand rejected under 35 U.S.C. § 103 as obvious over Ateniese in view of Camenisch. Finally, claims 13-14 and 16-17 stand rejected under 35 U.S.C. § 103 as obvious over Ateniese in view of Camenisch. \

The examiner's rejections are respectfully traversed.

The Ateniese reference disclose (see page 5, lines 14-17) a signature scheme where all of the members of the subgroup sign on the same message *m*. In contrast, in accordance with applicant's invention, each member is able to sign its own message *m*. Such a distinction is brought out by the language of the claims wherein it is stated in both of applicant's independent claims 1 and 18:

> an anonymous signing section for authorizing individual data using the secret information.

As such, applicant's claims readily distinguish over the primary Ateniese reference. In order for a reference to be utilized as an anticipatory reference under the provisions of 35 U.S.C. § 102, the reference must disclose each and every claim limitation. This is certainly not the case here, and thus the Sec. 102 rejection must be withdrawn.

Moreover, as disused in Sec. 10 of Ateniese (see line 4-5 of Sec. 10), members of the subgroup need to agree on a common random, one-time base before signing. In applicant's invention, such a common agreement is not needed and each member can independently sign their message.

As to the Ramzan reference, there is described a voting system using a Group Blind signature scheme. The subsystem generates his signature and gives it to the participant subsystem. The participant subsystem sends the vote with the signature to the manager subsystem to the reception subsystem, and the reception subsystem accept the vote if the vote bears the correct signature of the manager subsystem. The anonymity of the system is based n the fact that the vote of any participant subsystem carries only the signature of the manager subsystem. Therefore, the participant can not be identified. As may thus be seen, Ramzan does not teach the method of a participant subsystem comprising an anonymous signing section using a participant's secret key. As such, Ramzan, taken singly or even combined with Ateniese does not make our a *prima facie* case of obviousness under the provisions of 35 U.S.C. § 103.

Moreover, it should be noted that in the scheme of Ramzan, the manager subsystem can freely generate his signature and submit multiple votes, where in applicant's invention such a misuse of the system is thwarted.

The arguments set forth above are made with respect to the independent claims 1 and 18. As discussed above, these claims are deemed patentable over the prior art. Applicant's dependent claims are likewise deemed patentable, by virtue of their dependency, at least for the reasons set forth above in connection with the independent claims from which they depend.

Conclusions:

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a

check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date 1-3-05 By _____

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257